



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,302	12/04/2003	Brian Francis Cox	112025-0530	7927

24267 7590 01/25/2007
CESARI AND MCKENNA, LLP
88 BLACK FALCON AVENUE
BOSTON, MA 02210

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2131

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/728,302	Applicant(s) COX ET AL.	
	Examiner Christian La Forgia	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 December 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 December 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>3/9/04</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-24 have been presented for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 09 March 2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statement.

Drawings

3. Figures 1 and 4 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the examiner does not accept the changes, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

4. The use of the trademark Cisco Systems has been noted on page 13 and 14 in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.
5. Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 18-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As per claims 18-23, merely claimed as means for where the means is implemented in software representing a computer listing *per se*, that is, descriptions or expressions of such a program and that is, descriptive material *per se*, non-functional descriptive material, and is not statutory because it is not a physical “thing” nor a statutory process, as there are not “acts” being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed aspects of the invention which permit the computer program’s functionality to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer, the program itself is not a process, without the computer-readable medium needed to realize the computer program’s functionality. In contrast, a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer program and the medium which permit the computer program’s functionality to be realized, and is thus statutory. **Warmerdam**, 33 F.3d at 1361, 31 USPQ2d at 1760. **In re Sarkar**, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a).

8. Page 25, lines 29-30 of the Specification of the instant application describes that the present invention can be implemented as software, thereby rendering the “means for” language in claims 18-23 as computer software. *In re Donaldson Co.*, 16 F.3d 1189, 29 USPQ2d 1845 (Fed. Cir. 1994), decided that

Art Unit: 2131

the "broadest reasonable interpretation" that an examiner may give means-plus-function language is that statutorily mandated in paragraph six. Accordingly, the PTO may not disregard the structure disclosed in the specification corresponding to such language when rendering a patentability determination.

See MPEP § 2181 also. Therefore, giving the claims their broadest reasonable interpretation, while keeping the structure disclosed in the specification in my mind, one of ordinary skill in the art would construe claims 18-23 as representing a computer program *per se*.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-4, 14, 18, and 24 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0158735 to Roese, hereinafter Roese.

11. As per claims 1, 14, 18, and 24, Roese teaches a method, an intermediate node, an apparatus, and a computer-readable medium for implementing port-based network access control at a shared media port in an intermediate node, the shared media port being coupled to a plurality of client nodes, the method comprising:

partitioning the shared media port into a plurality of logical subinterfaces (paragraph [0012], i.e. an authenticator includes one or more sets of controlled and uncontrolled ports), each logical subinterface dedicated to providing access to a different network or subnetwork

accessible through the intermediate node (paragraph [0012], i.e. upon authentication, the logical controlled port is enabled and the supplicant is granted access to those network services);

receiving a data packet at the shared media port from a first client node (Figure 3 [block 250], paragraph [0028], i.e. receiving the packets);

associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces (Figure 3 [block 251], paragraph [0028], i.e. inspect the packets for reserved MAC address and 802.1X formats);

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (Figure 3 [block 255], paragraph [0028], i.e. rendering an authenticated/not authenticated decision); and

if the first client node is determined to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (Figure 3 [block 255], paragraph [0028], i.e. rendering an authenticated/not authenticated decision), forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork (paragraph [0012], i.e. upon authentication, the logical controlled port is enabled and the supplicant is granted access to those network services).

12. Regarding claim 2, Roes teaches performing at least one of dropping the received data packet or reclassifying the received data packet to a different logical subinterface (paragraph [0028], i.e. unrecognized packets are discarded), if the first client node is determined not to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (paragraph [0028], i.e. decision rendered that packet is not authenticated).

13. Regarding claim 3, Roese teaches wherein the first logical subinterface's dedicated network or subnetwork is a virtual private network (VPN) (paragraphs [0023], [0025]).

14. Regarding claim 4, Roese teaches wherein a logical subinterface in the plurality of logical subinterfaces is dedicated to providing access to the Internet (Figures 1 [blocks 105a, 105b], 2, paragraph [0023]).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

16. Claims 5, 8, 9, 11, 13, 15, 17, 19, and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roese in view of U.S. Patent Application Publication No. 2005/0055570 to Kwan et al., hereinafter Kwan.

17. Regarding claims 5, 17, and 19, Roese teaches wherein the step of determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork further comprises:

parsing a source media access control (MAC) address from the received data packet (Figure 3 [block 251], paragraph [0028], i.e. inspect the packets for reserved MAC address and 802.1X formats);

comparing MAC address and 802.1X formats with stored known Ethernet and authentication packet types (Figure 3 [block 251], paragraph [0028]);

identifying an authentication state stored in the indexed MAC-filter entry (paragraph [0029], i.e. state must be kept on sessions relayed by either MAC address or internal 802.1X protocol); and

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork based on the stored authentication state (Figure 3 [blocks 255], paragraphs [0028]-[0029], i.e. rendering an authenticated/not authenticated decision).

18. Roese does not disclose indexing an entry in a MAC filter to discover authentication state information.

19. Kwan discloses using a MAC filter to control the authentication state of users (paragraphs [0005], [0012], [0013]).

20. It would have been obvious to one of ordinary skill in the art at the time the invention was made to index an entry in a MAC filter associated with the shared media port based on the value of the parsed source MAC address, and storing the authentication state in the indexed MAC-filter entry, since Kwan states at paragraph [0014] that MAC authentication provides network security in a more efficient manner than conventional solutions.

21. Regarding claims 8 and 21, Roese does not teach wherein the step of associating the received data packet with the first logical subinterface, further comprises locating an entry in a routing table configured to store routing information associated with the received data packet;

Art Unit: 2131

and associating the received data packet with the first logical subinterface based on the contents of the routing-table entry.

22. Kwan discloses receiving packets and routing the information to the appropriate output port based on information such as the destination address (Figure 2, paragraphs [0033]-[0034]).

23. It would have been obvious to one of ordinary skill in the art at the time the invention was made to locate an entry in a routing table configured to store routing information associated with the received data packet; and associate the received data packet with the first logical subinterface based on the contents of the routing-table entry, since Kwan states at paragraph [0033] that including routing information on a network access device allows a user, such as a system administrator, to reconfigure the network access device and adjust its operating parameters, thereby controlling who can access the data communications network (paragraph [0008]).

24. Regarding claims 9, 15, and 22, Roese teaches receiving an authentication request from the first client node at the shared media port (Figure 3 [block 250], paragraph [0028], i.e. receiving the packets);

forwarding the received authentication request to an authentication service (Figure 3 [block 252], paragraph [0028]);

receiving a response from the authentication service, the response identifying an authentication state associated with the first client node (Figure 3 [block 256], paragraph [0028]);
and

storing the authentication state into which the source MAC address was copied (paragraphs [0028]-[0029]).

25. Roese does not disclose in response to receiving the authentication request, creating a MAC filter associated with the shared media port if the MAC filter has not already been created; copying a source MAC address stored in the received authentication request into an appropriate entry in the MAC filter; and storing the authentication state into the MAC-filter entry.

26. Kwan discloses storing the MAC addresses in a local or global memory (paragraph [0046]), which are used as the control when an authentication request is received (paragraph [0053]).

27. It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a MAC filter in response to receiving the authentication request, copying the source MAC address into the MAC-filter entry, and eventually storing its authentication state, since Kwan states at paragraph [0014] that MAC authentication provides network security in a more efficient manner than conventional solutions.

28. With regards to claims 11 and 23, Roese teaches wherein the received authentication request is an 802.1X authentication request (paragraph [0028], i.e. 802.1X EAP (Extensible Authentication Protocol)).

29. With regards to claim 13, Roese teaches sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node's authentication state

Art Unit: 2131

changes from an authenticated state to an unauthenticated or unknown state (paragraph [0029], i.e. tracking state changes via a tracking function).

30. Claims 6 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roesse in view of Kwan as applied to claim 5 above, and further in view of U.S. Patent Application Publication No. 2005/0177865 to Ng et al., hereinafter Ng.

31. With regards to claim 6, Roesse and Kwan do not teach wherein the MAC filter is organized as a hash table.

32. Ng discloses wherein the state information has been stored using a hash function (paragraph [0080]).

33. It would have been obvious to one of ordinary skill in the art at the time the invention was made to organize the MAC filter as a hash table, since one of ordinary skill in the art would recognize that the MAC addresses were being used as authentication means it would be necessary to store the address in a protected format, similar to how Unix systems store user passwords in a hashed file, to prevent unauthorized users from acquiring the MAC addresses if the intermediate node was ever compromised.

34. With regards to claim 10, Roesse and Kwan do not teach indexing an entry in the MAC filter based on the result of applying a hash function to the source MAC address; and storing the source MAC address at the indexed MAC-filter entry.

35. Ng discloses hashing local node information along with the state information for authentication purposes (paragraph [0080]).

36. It would have been obvious to one of ordinary skill in the art at the time the invention was made to index an entry in the MAC filter based on the result of applying a hash function to the source MAC address and store the source MAC address at the indexed MAC-filter entry, since one of ordinary skill in the art would recognize that the MAC addresses were being used as authentication means it would be necessary to store the address in a protected format, similar to how Unix systems store user passwords in a hashed file, to prevent unauthorized users from acquiring the MAC addresses if the intermediate node was ever compromised.

37. Claims 7, 16, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roese in view of U.S. Patent Application No. 2004/0208151 to Haverinen et al., hereinafter Haverinen.

38. Regarding claims 7, 16, and 20, Roese does not teach parsing a destination Internet Protocol (IP) address from the received data packet; comparing the parsed destination IP address to one or more IP addresses stored in an IP filter associated with the shared media port; and if the parsed destination IP address matches an IP address stored in the IP filter, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork, even if the first client node is determined not to be authenticated to communicate over that network or subnetwork.

39. Haverinen teaches parsing a destination Internet Protocol (IP) address from the received data packet (Figure 1 [blocks 104], paragraph [0029], i.e. receive IP address);

comparing the parsed destination IP address to one or more IP addresses stored in an IP filter associated with the shared media port (Figure 1 [block 105], paragraph [0029], i.e. IP authentication protocol); and

if the parsed destination IP address matches an IP address stored in the IP filter, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork (paragraph [0029], i.e. successful IP authentication protocol allows access controller to relay data packets of terminal device), even if the first client node is determined not to be authenticated to communicate over that network or subnetwork (Figure 1 [block 102], i.e. no IEEE 802.1X authentication).

40. It would have been obvious to one of ordinary skill in the art at the time the invention was made to perform an open systems authentication protocol, since Haverinen states at paragraph [0004] that using an open systems authentication protocol, specifically one focused on the third layer of the OSI model, allows wireless users to authenticate and access network resources, thereby allowing users the freedom to access network resource whenever and where ever they would like.

41. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roese in view of Kwan as applied to claim 9 above, and further in view of U.S. Patent No. 6,891,819 to Inoue et al., hereinafter Inoue.

42. With regards to claim 12, Roese and Kwan do not teach sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node fails to authenticate at the shared media port a predetermined number of times.

Art Unit: 2131

43. Inoue discloses tracking the number of times a user has failed authentication and providing an indication that said account has failed authentication a predetermined number of times (Figures 12-14, 18 and 19, column 12, lines 45-67, column 13, lines 22-46, column 17, lines 53-59).

44. It would have been obvious to one of ordinary skill in the art at the time the invention was made to send an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node fails to authenticate at the shared media port a predetermined number of times, since Inoue states at column 3, lines 1-6 that tracking the number an authentication fails helps to prevent the improper acquisition of user or network information since reaching the threshold of improper authorization attempts is a clear indicator that the user account or mobile system has been compromised.

Conclusion

45. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

46. The following patents are cited to further show the state of the art with respect to 802.1X authentication techniques, such as:

United States Patent Application Publication No. 2005/0111466 to Kappes et al., which is cited to show 802.1X authentication based on a token.

United States Patent Application Publication No. 2003/0217122 to Roese et al., which is cited to show 802.1X authentication for mobile terminals.

United States Patent Application Publication No. 2004/0172559 to Luo et al., which is cited to show 802.1X protocol based multicasting control.

United States Patent Application Publication No. 2004/0073793 to Takeda, which is cited to show 802.1X authentication for mobile terminals.

United States Patent Application Publication No. 2006/0277187 to Roese et al., which is cited to show 802.1X authentication for mobile terminals.

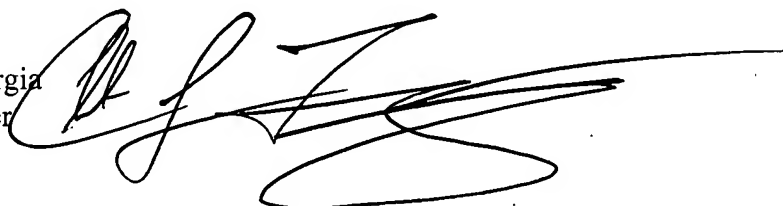
United States Patent Application Publication No. 2005/0080921 to Lu, which is cited to show implementing handshaking between 802.1X-based devices.

47. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

48. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

49. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

A handwritten signature in black ink, appearing to read 'C. LaForgia', is written over the printed name and title of the examiner.

Art Unit: 2131

clf